## FRANKLIN GRAY PATENTS, LLC
### ROBERT H. FRANTZ, REGISTERED US PATENT AGENT

# FACSIMILE TRANSMISSION

**RECEIVED**
**CENTRAL FAX CENTER**

**JUN 1 9 2006**

TO:   Examiner Shahin Mizan          FROM:    Robert H. Frantz
      U.S. Patent and Trademark Office          Franklin Gray Patents, LLC
      GAU  2132                                 Tel: 405-812-5613
      Fax: 571-273-8300 (Central Fax Server)    Fax: 405-440-2465

DATE:      June 19, 2006

PAGES:     19 (inclusive)


In re the Application of:

Anthony Edward Martinez                    )

Serial Number: 10/082,744                  )                          Group: 2132

Docket Number: AUS920020005US1             )                 Examiner: Shahin Mizan

Filed on: 2/21/2002                        )

For: "Electronic Password Wallet"          )


---

**Certificate of Transmission under 37 CFR §1.8**

I hereby certify that this correspondence is being facsimile transmitted to the Patent and Trademark Office on:

DATE: *June 19, 2006*     SIGNATURE: */ Robert Frantz /*

Robert H. Frantz, Reg. No. 42,553

---

(Modified) PTO/SB/17 (12-04v2)

# FEE TRANSMITTAL
## for FY 2005

*Effective 12/08/2004. Patent fees are subject to annual revision.*

| Complete if Known | |
|---|---|
| Application Number | **10/082,744** |
| Filing Date | 02/21/2002 |
| First Named Inventor | Anthony Edward Martinez |
| Examiner Name | Shahin Mizan |
| Art Unit | 2132 |
| Attorney Docket No. | AUS920020005US1 |

☐ Applicant claims small entity status. See 37 CFR 1.27

**TOTAL AMOUNT OF PAYMENT**    (*) $ 500.00

## METHOD OF PAYMENT *(check all that apply)*

☐ Check    ☐ Credit card    ☐ Money Order    ☐ None    ☐ Other (please identify): _____

☒ Deposit Account:

Deposit Account Number: **09-0447**    Deposit Account Name: **IBM Corporation**

The Director is authorized to: *(check all that apply)*

☒ Charge fee(s) indicated below
☒ Charge any additional fee(s) or any underpayment of fee(s) under 37 CFR 1.16 and 1.17

☐ Charge fee(s) indicated below, **except for the filing fee**
☒ Credit any overpayments

## 1. BASIC FILING, SEARCH, AND EXAMINATION FEES
### FEE CALCULATION

| Application Type | FILING FEES Fee ($) | Small Entity Fee ($) | SEARCH FEES Fee ($) | Small Entity Fee ($) | EXAMINATION FEES Fee ($) | Small Entity Fee ($) | Fees Paid ($) |
|---|---|---|---|---|---|---|---|
| Utility | 300 | 150 | 500 | 250 | 200 | 100 | _____ |
| Design | 200 | 100 | 100 | 50 | 130 | 65 | _____ |
| Plant | 200 | 100 | 300 | 150 | 160 | 80 | _____ |
| Reissue | 300 | 150 | 500 | 250 | 600 | 300 | _____ |
| Provisional | 200 | 100 | 0 | 0 | 0 | 0 | _____ |

## 2. EXCESS CLAIM FEES
### FEE DESCRIPTION

| | Fee ($) | Small Entity Fee ($) |
|---|---|---|
| ● Each claim over 20 or, for reissues, each claim over 20 and more than in the original patent | 50 | 25 |
| ● Each independent claim over 3 or, for Reissues, each independent claim more than in the original patent | 200 | 100 |
| ● Multiple dependent claims | 360 | 180 |

| Total Claims | | Extra Claims | | Fee($) | | Fee Paid ($) | Multiple Dependent Claims Fee($) Fee Paid ($) |
|---|---|---|---|---|---|---|---|
| | - 20 or HP= | | X | 50 | = | | 360 x |

*HP = highest number of total claims paid for, if greater than 20*

| Indep. Claims | | Extra Claims | | Fee($) | | Fee Paid ($) |
|---|---|---|---|---|---|---|
| | - 3 or HP= | | X | 200 | = | |

*HP = highest number of total claims paid for, if greater than 3*

## 3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41 (a)91)(G) and 37 CFR 1.16(s).

| Total Sheets | | Extra Sheets | | Number of each additional 50 or fraction thereof | | Fee($) | | Fee Paid ($) |
|---|---|---|---|---|---|---|---|---|
| | - 100 = | | /50 = | (round up to a whole number) | X | 250 | = | |

## 4. OTHER FEE(S)

Fees Paid ($)

Non-English Specification, $130 fee

Other: _____ Fee for filing a Brief in support of an Appeal (41.20(b)(2)    $500.00

| SUBMITTED BY | | | | |
|---|---|---|---|---|
| Name | Robert H. Frantz | Registration No. | 42,553 | Telephone 405-812-5613 |
| Signature | /Robert Frantz/ | | | Date 6/ 19 / 2006 |

# 𝔍𝔫 𝔱𝔥𝔢 𝔘𝔫𝔦𝔱𝔢𝔡 𝔖𝔱𝔞𝔱𝔢𝔰 𝔓𝔞𝔱𝔢𝔫𝔱 𝔞𝔫𝔡 𝔗𝔯𝔞𝔡𝔢𝔪𝔞𝔯𝔨 𝔒𝔣𝔣𝔦𝔠𝔢

In re the Application of:

| | | |
|---|---|---|
| Anthony Edward Martinez | ) | |
| Serial Number: 10/082,744 | ) | Group: 2132 |
| Docket Number: AUS920020005US1 | ) | Examiner: Shahin Mizan |
| Filed on: 2/21/2002 | ) | |
| For: "Electronic Password Wallet" | ) | |

## APPEAL BRIEF

*Real Party in Interest per 37 CFR §41.37(c)(1)(i)*

The subject patent application is owned by International Business Machines Corporation of Armonk, NY.

*Related Appeals and Interferences per 37 CFR §41.37(c)(1)(ii)*

None.

*Status of Claims per 37 CFR §41.37(c)(1)(iii)*

Claims 1 - 19 are finally rejected. The rejections of Claims 1 - 19 are appealed.

*Status of Amendments after Final Rejections per 37 CFR §41.37(c)(1)(iv)*

No amendments to the claims have been submitted or entered after final rejections.

*Summary of the Claimed Subject Matter per 37 CFR §41.37(c)(1)(v)*

The present invention provides a method and system for providing a secure field value retrieval and entry on a computing platform's display device, such as username and password entry fields, through:

    (a)    providing to a plurality of application programs an interface (#34 in Fig. 3; paras. 0045 - 0046) to request application-specific passwords, said plurality of application programs including at least one web browser program (Fig. 3 #26, para. 0045), and at least one non-browser program (Fig. 3 #23, para. 0045);

    (b)    receiving a request from an application program via said interface for input of an application-specific password (App_ID, User_ID, Mstr_PW in Fig. 3, para.0046);

    (c)    receiving a computing context indicator regarding at least a position of an original entry point for a password as displayed by said requesting application program ("screen location" in para. 0046);

    (d)    displaying a user first dialogue to receive a master key value from a user (#42 in Fig. 4, para. 0051), said user dialogue being displayed in a position so as to overlay (para. 0065, #62 and #65 in Fig. 6) said original entry point for a password as displayed by said requesting application program;

    (e)    determining if said master key value is a correct master key value (#43 in Fig. 4, paras 0052 and 0053);

    (f)    retrieving a plurality of field values from a secure field value store which are associated with said requesting application program, said activated field and a user identification (#31 in Fig. 3, paras. 0054 and 0068);

    (g)    displaying to a user a second dialogue to receive a selection by said user from said retrieved plurality of field values (#65 in Fig. 6c, para. 0068); and

    (h)    automatically entering said selected field value into said original entry point for said requesting application program (#48 in Fig. 4, paras. 0057 and 0069).

Claim 1 sets forth this method, and Claim 7 sets forth an corresponding computer readable medium encoded with software for performing this method. Claim 13 sets forth a system for performing these corresponding functions.

***Grounds for Rejection For Which Review is Sought per 37 CFR §41.37(c)(1)(vi)***

Review by the Board of the rejections of Claims 1 - 19 under 35 U.S.C. §102(b) as being anticipated by published U.S. patent 6,182,229 to Nielsen (hereinafter "Nielsen") is requested.

***Arguments per 37 CFR §41.37(c)(1)(vii)***

<u>Rejections of Claims 1 - 19 under 35 U.S.C. §102(b) over Nielsen</u>

Claims 1, 7, and 13 are independent method, software-encoded media, and system claims, respectively. All other claims depend from one of these claims.

Appellants believe the following errors have been made in arriving at the final rejection of claims 1, 7, and 13:

 (a) improperly equating a site server with an application program;

 (b) improperly reading our disclosure into the disclosure of the cited art regarding overlaying a dialog box;

 (c) incorrectly interpreting the cited art regarding the discrimination between multiple passwords indexed to the same web site or application program; and

 (d) issuing a 102 rejection which is supported by reasoning which likely should be supporting a 103 rejection because it relies upon inherent or common practice modifications to the actual teachings, and it relies upon reordering of steps in a process.

A. <u>Improperly Equating a Site Server with an Application Program.</u>

We have claimed certain functionality relative to application programs, not client-server or browser-server arrangements, including providing an interface to request *application-specific* passwords to *at least one non-browser program*, receiving such a request *from an application program* for input of an *application-specific* password, and receiving a computing context indicator regarding a position of an original entry point for a password as displayed by the requesting *application program*.

In this context, we are referring to an "application program" using the conventional meaning in the art, such as the definition from http://www.whatis.com, a information technology industry reference web site:

> **Application Program:** An application program (sometimes shortened to
> application) is any program designed to perform a specific function
> directly for the user or, in some cases, for another application program.
> Examples of application programs include word processors; database
> programs; Web browsers; development tools; drawing, paint, and image
> editing programs; and communication programs. Application programs
> use the services of the computer's operating system and other supporting
> programs. The formal requests for services and means of communicating
> with other programs that a programmer uses in writing an application
> program is called the application program interface (API)

So, to be certain that our definition and use of the term includes these applications besides a web browser, we have specified that our application programming interface (API) is provided to at least one non-browser program.

Nielsen is directed towards password handling between a web browser and a server, where the resource which is being logged into is being run or executed by the server. Our examples of other non-browser application programs, such as word processors, are "locally" executed by the user's own computer, and thus could also be described as "off line" applications.

Because Nielsen is not directed towards non-browser-server arrangements, Nielsen is silent regarding providing an open application interface such that both web browsers and non-browser applications alike can access the same password wallet.

The rationale for the rejections is erroneously based upon a holding that an API to a non-browser application program (our claim) is equivalent under 35 U.S.C. §102 to a web browser/server arrangement (the cited art). For this reason, the rejections of claims 1, 7, and 13 should be reversed.

B.      Improperly Reading Our Disclosure into the Disclosure of the Cited Art

       Regarding Overlaying a Dialog Box

We have claimed that upon an attempt to login to a password-protected application program, the invention "overlays" a user dialog on top of the normal username/password dialog of the application program:

> . . .  displaying a user first dialogue to receive a master key value from a user, said user dialogue being displayed in a position so as to overlay said original entry point for a password as displayed by said requesting application program; . . .

For better interpretation of this visual effect, we have provided an illustration of such an overlay.

Nielsen, however, does not overlay the normal login dialog, nor does Nielsen provide a secondary login dialog for the user to select from or complete, but instead Nielsen inhibits the display of the login dialog entirely, favoring to automatically enter the username and password:

> · . . . The password management system of the present invention maintains a database of passwords and user IDs as they are known to the remote sites. This information is encrypted using the master password. **When a request for authentication is received, the system intercepts the request, inhibiting the browser from displaying the usual authentication form,** decrypts the needed password and user ID using the master password, and forwards the decrypted password and user ID to the requesting remote site. The remote site receives the decrypted password and user ID in the same way it would if this information had been input into the usual authentication form at client computer system 10. (Col 3 line 67 - col. 4 line 6, emphasis added by appellants)
>
> . . .
>
> Browser programs will generally respond to an authentication request by displaying an authentication form having entry fields for the user's ID and password. However, the password management system intercepts the request and responds to the authentication request at step 310 by **inhibiting display of this form. Instead, the password management**

system attempts to respond to the authentication request
automatically (Col. 4 lines 52 - 59, emphasis added by appellants)

In fact, Nielsen's invention provides their master password dialog primarily during first-time login (e.g. "registration), but not normally during subsequent logins:

> At step 312, the database of FIG. 2 is scanned for an entry having the
> URL of the web site sending the authentication request. If an entry is
> found, the password management system decrypts the password and
> user ID information using the master password as a key at step 314. If
> the master password was not entered at step 302 due to the preference
> setting, the user is prompted for it now. If at step 312, no URL
> corresponding to the remote server requesting authentication is found,
> the password management system carries out a series of steps related to
> registration that are discussed in reference to FIG. 4. At step 316, the
> password and user ID information decrypted at step 314 is sent to the
> remote site as if this information had been entered in the usual
> authentication form. (Col. 4 lines 60 - 67)

As such, Nielsen fails to disclose as required by 35 U.S.C. §102 our claimed step or element of a master password wallet dialog overlaid on the normal login dialog for a non-browser application program. For this reason, the rejection of claims 1, 7, and 13 are erroneous and should be reversed.

C.    Incorrectly Interpreting the Cited Art Regarding the Discrimination Between
      Multiple Passwords Indexed to the Same Web Site or Application Program

We have claimed the ability or functionality which allows the master password wallet to manage passwords for multiple users of the same website or application program.  As such, our passwords are indexed not only to the application program with which they are associated, but also they are indexed to a user with whom they are associated:

> . . .   retrieving a plurality of field values from a secure field value store which are
> associated with said requesting application program, said activated field and a user
> identification;
>       displaying to a user a second dialogue to receive a selection by said user from
> said retrieved plurality of field values; and . . .

In the rationale for the final rejections, it was held that Nielsen teaches this indexing of usernames and passwords by website and by user at col. 4, line 1.  It is important to keep in mind that for a given user, there may be multiple username (or User-ID) values for multiple websites. For example, for a user whose full real name is "Bob Smith", he may have a User-ID of "bsmith" at Yahoo.com, another User-ID of "BobSmith123" at Amazon.com, and a third User-ID of "BobbyS-HarleyRider" at a motorcycling enthusiasts web site.  As such, there are four, not three, distinctive fields needed for each record in the password database to index according to our invention: (1) an identifier of the actual user to the invention or password wallet (in this example "Bob Smith"), (2) an identifier of the application program or web site to which this user wants access (e.g. WordPerfect, PowerPoint, Amazon.com, etc.), (3) the User-ID value needed to log into the application or web site (in this example "bsmith" or "BobbyS-HarleyRider"), and (4) the password associated with this User-ID at this web site or for this application program.

So, Nielsen has disclosed a database having User-IDs, but there is no provision for further indexing (e.g. adding the fourth needed field of the password wallet user's universal name or real name) to the user.  This makes Nielsen's invention inoperable for two different users, say Bob Smith and his wife, Betty Smith, to use the same wallet (e.g. the same password database).

If the interpretation of Nielsen's disclosure were correct, it would be reasonable to assume that Nielsen would include further disclosure to support the display dialogs necessary to allow a user to pick which User-ID to use when logging into a web site or application program where two or more users are known to access.  However, Nielsen provides no illustration of

such, and does not describe such a discrimination process.

For these reasons, the rationale for the final rejections of claims 1, 7, and 13 are in error, and reversal of the rejections is requested.

D.     Improper Support of a Rejection Under 35 U.S.C. §102 Based Upon Inherent or Common Practice Modifications to the Actual Teachings, and Based Upon Undisclosed Re-ordering of Steps of the Cited Art

In response to Appellants' amendment and remarks following the first Office Action in the examination of this application, the examiner has maintained many points of the rejection on the basis of certain "inherent" functions of the cited art, and reasoning that certain differences between our claims and the details of the Nielsen disclosure are just "common practice" implementation choices. The examiner has stated that certain actions have been "implied", which leads to other steps which "can be" performed.

However, the Court has held that inherent teaching to anticipate a claim element or step requires more than just capability to be modified in cases such as *In re* Robertson (169 F.3d 743, 49 USPQ2d 1949, Fed. Cir. 1999) and *In re* Oelrich (666 F.2d 578, 581, 212 USPQ 323, 326, C.C.P.A. 1981).

This holding applies to the present patent application, whereas Nielsen might possibly have been disclosed as having certain design changes to utilize an open API, or to reorder their steps to the approximate order of our steps, etc., but Nielsen did not disclose such optional embodiments. Whereas these embodiments bring about specific functionality not present in the browser-server arrangement of Nielsen's disclosure, then the functionality is not inherent in Nielsen's disclosure.

For these reasons, the rejections of claims 1, 7, and 13 were erroneous, and reversal of the rejections is requested.
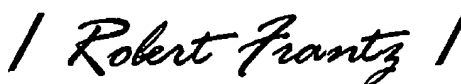
### Rejections of Claims 2 - 6, 8 - 12, and 14 - 19 under 35 U.S.C. §102(b) over Nielsen

Claims 2 - 6 depend from Claim 1, Claims 8 - 12 depend from Claim 7, and Claims 14 - 19 depend from Claim 13. For the reasons as discussed in the foregoing paragraphs, Appellants request reversal of the rejections. All of these claims recite steps, elements, and limitations not taught by Nielsen.

With further respect to Claims 3, 9, and 15, wherein we have claimed the request for password is received from an application program (e.g. a non-browser program), it was reasoned that Nielsen teaches their invention "could be" incorporated into a web browser. It was not acknowledged in the same reasoning, however, that the alternate embodiment disclosed at col. 3, lines 53 - 60, was also referring to receiving the request from a web browser (not from a non-browser program), albeit the functionality of Nielsen's invention would be embodied in an applet or HotJava code segment. In either embodiment, the *request* for the password is coming from a web browser, not a non-browser application program.

For these reasons, Appellants request the reversal of the rejections of claims 2 - 6, 8 - 12, and 14 - 19.

Respectfully,

/ Robert Frantz /

Robert H. Frantz, Reg. No. 42,553
Agent for Appellants      Tel: (405) 812-5613
**FRANKLIN GRAY PATENTS, LLC**

Franklin Gray Patents, LLC
P.O. Box 23324
Oklahoma City, OK 73127
Tel: 405-812-5613
Fax: 405-440-2465

## Claims Appendix
### *per 37 CFR §41.37(c)(1)(viii)*

### Clean Form of Amended Claims

Claim 1 (previously presented):

  A method within a computing platform of graphically providing a secure field value retrieval and entry, wherein said computing platform includes a display device, a field activation device and a user selection device, said method comprising:

    providing to a plurality of application programs an interface to request application-specific passwords, said plurality of application programs including at least one web browser program, and at least one non-browser program;

    receiving a request from an application program via said interface for input of an application-specific password;

    receiving a computing context indicator regarding at least a position of an original entry point for a password as displayed by said requesting application program;

    displaying a user first dialogue to receive a master key value from a user, said user dialogue being displayed in a position so as to overlay said original entry point for a password as displayed by said requesting application program;

    determining if said master key value is a correct master key value;

    retrieving a plurality of field values from a secure field value store which are associated with said requesting application program, said activated field and a user identification;

    displaying to a user a second dialogue to receive a selection by said user from said retrieved plurality of field values; and

    automatically entering said selected field value into said original entry point for said requesting application program.

Claim 2 (original):

  The method as set forth in Claim 1 wherein said step of displaying a user dialogue comprises receiving a user identification value.

Claim 3 (original):

  The method as set forth in Claim 1 wherein said step of retrieving a field value from a secure field value store which correlates to a computing context comprises retrieving a field value which is associated with an application program.

Claim 4 (original):

  The method as set forth in Claim 1 wherein said step of retrieving a field value from a secure field value store which correlates to a computing context comprises retrieving a field value which is associated with a web site.

Claim 5 (original):

  The method as set forth in Claim 1 wherein said step of retrieving a field value from a secure field value store which correlates to a computing context comprises retrieving a field value which is associated with a web form.

Claim 6 (original):

  The method as set forth in Claim 1 wherein said step of automatically entering said retrieved field value into said activated field comprises automatically entering a password value.

Claim 7 (previously presented):

A computer readable medium encoded with software for graphically providing
a secure field value retrieval and entry, wherein said computing platform
includes a display device, a field activation device and a user selection device,
said software causing the computing platform to perform the steps of:

provided to a plurality of application programs an interface to request
application-specific passwords, said plurality of application programs including at least
one web browser program, and at least one non-browser program;

receiving a request from an application program via said interface for input of an
application-specific password;

receiving a computing context indicator regarding at least a position of an original
entry point for a password as displayed by said requesting application program;

displaying a user dialogue to receive a master key value from a user, said user
dialogue being displayed in a position so as to overlay said original entry point for a
password as displayed by said requesting application program;

determining if said master key value is a correct master key value;

retrieving a field value from a secure field value store which is associated with
said requesting application program, said activated field and a user identification; and

automatically entering said retrieved field value into said original entry point for
said requesting application program.


Claim 8 (original):

The computer readable medium as set forth in Claim 7 wherein said software
for displaying a user dialogue comprises software for receiving a user
identification value.

Claim 9 (original):

  The computer readable medium as set forth in Claim 7 wherein said software
  for retrieving a field value from a secure field value store which correlates to a
  computing context comprises software for retrieving a field value which is
  associated with an application program.

Claim 10 (original):

  The computer readable medium as set forth in Claim 7 wherein said software
  for retrieving a field value from a secure field value store which correlates to
  a computing context comprises software for retrieving a field value which is
  associated with a web site.

Claim 11 (original):

  The computer readable medium as set forth in Claim 7 wherein said software
  for retrieving a field value from a secure field value store which correlates to
  a computing context comprises software for retrieving a field value which is
  associated with a web form.

Claim 12 (original):

  The computer readable medium as set forth in Claim 7 wherein said software
  for automatically entering said retrieved field value into said activated field
  comprises software for automatically entering a password value.

Claim 13 (previously presented):

A system for graphically providing a secure field value storage, retrieval and entry within a computing platform, wherein said computing platform includes a display device, a field activation device, a user selection device and a data storage medium, said system comprising:

an interface accessible by a plurality of application programs to request application-specific passwords, said plurality of application programs including at least one web browser program, and at least one non-browser program;

a request received from an application program via said interface for input of an application-specific password, including a computing context indicator regarding at least a position of an original entry point for a password as displayed by said requesting application program;

a secure field value store disposed within said data storage medium;

a user dialogue display on said display device adapted to receive a master key value from a user, said user dialogue being displayed in a position so as to overlay said original entry point for a password as displayed by said requesting application program;

a master key value evaluator for determining if a master key value entered via said user dialogue display is a correct master key value for said secure field value store;

a field value retriever for finding in and retrieving from said secure field value store a field value which is associated with said requesting application program and a user identification; and

a field value inputter for automatically entering said retrieved field value into said original entry point.

Claim 14 (original):

The system as set forth in Claim 13 wherein said user dialogue display is further adapted to receive a user identification value, and wherein said field value retriever is further adapted to find and retrieve a field value which is associated with a user identification value.

Claim 15 (original):

The system as set forth in Claim 13 wherein said step of retrieving a password from a secure field value store which correlates to a computing context comprises retrieving a field value which is associated with an application program.

Claim 16 (original):

The system as set forth in Claim 13 wherein said step of retrieving a field value from a secure field value store which correlates to a computing context comprises retrieving a field value which is associated with a web site.

Claim 17 (original):

The system as set forth in Claim 13 wherein said step of retrieving a field value from a secure field value store which correlates to a computing context comprises retrieving a field value which is associated with a web form.

Claim 18 (original):

The system as set forth in Claim 13 wherein said step of automatically entering said retrieved field value into said activated field comprises automatically entering a password value.

Claim 19 (original):

The system as set forth in Claim 13 where said field value store is a database.

<u>Serial No. 10/082,744</u>          <u>Anthony Edward Martinez</u>          <u>Page 16 of 17</u>

**Evidence Appendix**

*per 37 CFR §41.37(c)(1)(ix)*


No evidence has been submitted by applicant or examiner pursuant to 37 CFR §§1.130,

1.131, or 1.132.

## Related Proceedings Appendix
### *per 37 CFR §41.37(c)(1)(x)*

No decisions have been rendered by a court or the Board in the related proceedings as identified under 37 CFR §41.37(c)(1)(ii).